SCADA Field Device Protection Profile Project

Milestone 3: Security Objectives

This section identifies the security objectives for the TOE and the operating environment.

TOE Security Objectives

This section defines the security objectives that are to be addressed by the TOE.

O.ApplicationIntegrity	The TOE shall prevent an unauthorized user or device from modifying or deleting TOE application software. The TOE shall prevent an unauthorized user or device from modifying the TOE application configuration.
O.Audit	The TOE shall be capable of recording security related events.
O.Authentication	The TOE shall be capable of authenticating the identity of a user or device.
O.AccessControl	The TOE shall have an access control capability that restricts information access and operations to authenticated users and devices that are authorized for the requested information access or operation.
O.Confidentiality	The TOE shall be capable of establishing a secure communication channel with devices outside of the TOE boundary. This secure communication channel shall protect the confidentiality of the information sent in the channel.
O.DataFlowControl	The TOE shall be capable of preventing communication from a single or small set of IP addresses from stopping proper processing of communication received from other authenticated and authorized users and devices.
O.DataIntegrity	The TOE shall identify if data sent from an authenticated users or device has been modified prior to arriving at the TOE boundary. Modified data shall be rejected.
O.LimitFailedLoginAttempts	The TOE shall prevent an attacker from repeatedly guessing authentication credentials or exhaustively testing all possible authentication credentials.
O.ParameterChecking	The TOE shall identify and discard any communication that arrives at the TOE boundary that has parameters outside of the expected range.

Deleted: The TOE shall restrict information access and actions to authenticated users or devices.

Deleted: O.BoundaryChecking . The TOE shall identify and discard any communication that arrives at the TOE boundary that has parameters outside of the expected range.¶

Deleted: 03

O.ProtocolChecking	The TOE shall identify and discard any communication that arrives at the TOE boundary that violates the expected protocol format.
O.ReplayPrevention	The TOE shall identify and discard any communication that is a replay of previously received communication.
O.RoleBasedAccessControl	The TOE shall be capable of placing users and devices into roles and assigning authorization rights to the roles. The TOE shall support at a minimum an Administrator role and an Operator role.
O.SecureStartup	The TOE shall initiate all required security functions prior to accepting requests for information or requests for action.
O.StoredDataIntegrity	The TOE shall prevent an attacker from modifying or deleting data stored in the TOE.
O.SystemDiagnostics	The TOE shall be capable of performing diagnostic tests to verify the integrity of the operating system and application software.
O.SystemIntegrity	The TOE shall prevent unauthorized modification to the operating system software and configuration.

Security Objectives for the Operating Environment

This section defines the security objectives that are to be addressed by the operating environment.

OE.BackgroundCheck	All users shall undergo a background check consistent with the organizations policies and compliant with any applicable laws prior to be given a userID and credentials that provide access to the TOE.
OE.Identification	All users shall be uniquely identified with a userID. All devices shall be recognized in the TOE by a unique identifier.
OE.ReliableCommunication	Communication between the TOE and authorized subjects shall be reliable.
OE.StandardCrypto	The TOE shall use cryptologic algorithms and protocols that meet current NIST standards.

Deleted: uniquely identified

Deleted: by

Deleted: device name or fixed IP address

- - - End Draft Protection Profile Text - - -

Rationale

Section 6 of a Protection Profile requires a rationale that proves all the threats are addressed by the Security Objectives. The table below will be added to Section 6 when we are at that point, but it is useful to review now from two viewpoints.

1. A Security Objective may help identify a missing threat.
2. A Security Objective that does not meet any threats is an unnecessary threat and is removed from the Protection Profile.

Threat / Policy	Objectives Addressing Threat	Rationale
T.CredentialCracking An attacker may repeatedly try to guess authentication credentials in order to gain unauthorized access to the TOE.	**O.LimitFailedLoginAttempts** The TOE shall prevent an attacker from repeatedly guessing authentication credentials or exhaustively testing all possible authentication credentials. **O.Audit** The TOE shall be capable of recording security related events.	O.LimitedFailedLoginAttempts mitigates this threat by limiting the number of failed login attempts. An attacker would only be able to test a small number of the possible authentication credentials. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.
T.DataAlteration An attacker may intercept and modify communication sent to or from the TOE in an attempt to force an unauthorized action or affect the integrity of the TOE.	**O.DataIntegrity** The TOE shall identify if data sent from an authenticated user or device has been modified prior to arriving at the TOE boundary. Modified data shall be rejected. **O.BoundaryChecking** The TOE shall identify and discard any communication that arrives at the TOE boundary that has parameters outside of the expected range. **O.ProtocolChecking** The TOE shall identify and discard any communication that arrives at the TOE boundary that violates the expected protocol format. **O.Audit** The TOE shall be capable of recording security related events.	O.DataIntegrity mitigates this threat by determining if the data has been modified in transit and rejecting all altered data. O.BoundaryChecking and O.ProtocolChecking help to mitigate this threat by identifying data outside the expected range and data that violates the expected protocol. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.

Threat / Policy	Objectives Addressing Threat	Rationale
T.DataFlooding An attacker may send a large volume of data to the TOE to restrict the availability of the TOE. This threat may also be used to attempt to cause the TOE to improperly process data due to limited computing resources.	**O.DataFlowControl** The TOE shall be capable of preventing communication from a single or small set of IP addresses from stopping proper processing of communication received from other authenticated and authorized users and devices. **O.AccessControl** The TOE shall have an access control capability that restricts information access and operations to authenticated users and devices that are authorized for the requested information access or operation. **O.ProtocolChecking** The TOE shall identify and discard any communication that arrives at the TOE boundary that violates the expected protocol format. **O.ReplayPrevention** The TOE shall identify and discard any communication that is a replay of previously received communication. **O.Audit** The TOE shall be capable of recording security related events.	O.DataFlowControl mitigates this threat by preventing a single or small set of IP addresses from affecting the operation of the TOE for other IP addresses. O.AccessControl helps to mitigate this threat by rejecting requests from users and devices that attempt to exceed their authorizations. O.ProtocolChecking helps to mitigate this threat by discarding packets that violate the expected protocol. This could include packets that exceed the expected or maximum length. O.ReplayPrevention helps to mitigate this threat by discarding valid communication, which was from an authorized user or device and in the correct protocol format, that was recorded and replayed. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.
T.Eavesdropping An attacker may eavesdrop or sniff communication to or from the TOE thereby compromising the confidentiality of the information outside of the TOE.	**O.Confidentiality** The TOE shall be capable of establishing a secure communication channel with devices outside of the TOE boundary. This secure communication channel shall protect the confidentiality of the information sent in the channel.	O.Confidentiality mitigates this threat by providing a secure communication channel that protects the confidentiality of the data in the channel.

Threat / Policy	Objectives Addressing Threat	Rationale
T.EscalationOfPrivilege An attacker who has already gained authorized access to the TOE may attempt to increase its authorization rights by attacking the access control configuration.	**O.ApplicationIntegrity** The TOE shall prevent an unauthorized user or device from modifying or deleting TOE application software. The TOE shall prevent an unauthorized user or device from modifying the TOE application configuration. **O.AccessControl** The TOE shall have an access control capability that restricts information access and operations to authenticated users and devices that are authorized for the requested information access or operation. **O.RoleBasedAccessControl** The TOE shall be capable of placing users and devices into roles and assigning authorization rights to the roles. The TOE shall support at a minimum an Administrator role and an Operator role. **O.SecureStartup** The TOE shall initiate all required security functions prior to accepting requests for information or requests for action. **O.SystemIntegrity** The TOE shall prevent unauthorized modification to the operating system software and configuration. **O.Audit** The TOE shall be capable of recording security related events.	O.ApplicationIntegrity helps to mitigate this threat by preventing an attacker from modifying the TOE application to weaken access control protection. O.AccessControl helps to mitigate the threat by providing a means to limit authorization rights including the right to escalate privileges. O.RoleBasedAccessControl helps to mitigate this threat by making it easier to configure the TOE to limit who has the rights to escalate privileges. This right is typically limited to Administrators. O.SecureStartup helps to mitigate this threat by preventing an attacker from escalating privileges prior to the access control and other security controls being operational. O.SystemIntegrity helps to mitigate this threat by preventing an attacker from modifying the operating system to weaken access control protection. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.

Threat / Policy	Objectives Addressing Threat	Rationale
T.Hijacking An attacker may attempt to hijack an existing authorized session to gain the privileges of the user or device in the existing session.	**O.Confidentiality** The TOE shall be capable of establishing a secure communication channel with devices outside of the TOE boundary. This secure communication channel shall protect the confidentiality of the information sent in the channel. **O.DataIntegrity** The TOE shall identify if data sent from an authenticated source has been modified prior to arriving at the TOE boundary. Modified data shall be rejected. **OE.Identification** All users shall be uniquely identified with a userID. All devices shall be uniquely identified by device name or fixed IP address. **O.Audit** The TOE shall be capable of recording security related events.	O.Confidentiality mitigates this threat by preventing an attacker from selectively modifying data to hijack a session. Any encrypted bit that is modified will cause approximately 50% of the surrounding bits to be modified resulting in communication to appear as random data. An attacker will also be unable to send new encrypted requests to the TOE because it lacks the crypto keys. O.DataIntegrity mitigates this threat by identifying any changes to communication sent from an authorized source. An attacker will also be unable to send a new request to the TOE because the data integrity checks will fail. OE.Identification helps mitigate this threat by requiring the source to be uniquely identified. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.
T.MalformedData An attacker may attempt to compromise the availability or integrity of a TOE by sending malformed data to the TOE. Malformed data is data that does not comply with the expected protocol. It could be values outside of the permitted range, random modifications of the protocol, or data generated using protocol fuzzing tools.	**O.BoundaryChecking** The TOE shall identify and discard any communication that arrives at the TOE boundary that has parameters outside of the expected range. **O.ProtocolChecking** The TOE shall identify and discard any communication that arrives at the TOE boundary that violates the expected protocol format. **O.DataIntegrity** The TOE shall identify if data sent from an authenticated user or device has been modified prior to arriving at the TOE boundary. Modified data shall be rejected. **O.Audit** The TOE shall be capable of recording security related events.	O.BoundaryChecking helps mitigate this threat by discarding any data that includes parameters outside of the expected range. O.ProtocolChecking helps mitigate this threat by discarding any data that is not in the expected protocol format. O.DataIntegrity mitigates this threat from all attackers except an authenticated and authorized source by identifying and discarding any changes to data. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.

Deleted: 03

Threat / Policy	Objectives Addressing Threat	Rationale
T.Reconnaissance An attacker may attempt to gather information about the TOE, the TOE configuration, or information in the TOE for use in a future attack or to compromise the confidentiality of the TOE information.	**O.Authentication** The TOE shall be capable of authenticating the identity of a user or device. The TOE shall restrict information access and actions to authenticated users or devices. **O.AccessControl** The TOE shall have an access control capability that restricts information access and operations to authenticated users and devices that are authorized for the requested information access or operation. **O.Confidentiality** The TOE shall be capable of establishing a secure communication channel with devices outside of the TOE boundary. This secure communication channel must protect the confidentiality of the information sent in the channel. **OE.Identification** All users shall be uniquely identified with a userID. All devices shall be uniquely identified by device name or fixed IP address. **O.Audit** The TOE shall be capable of recording security related events.	OE.Identification and O.Authentication help mitigate this threat by requiring all users and devices to identify and authenticate themselves before gaining any information from the TOE. An attacker would need to gain a set of valid credentials to implement this threat. O.AccessControl helps mitigate this threat by implementing restrictions on what information a user or device can access. O.Confidentiality mitigates this threat if an attacker is monitoring communication on the network similar to T.Eavesdropping. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.
T.Replay An attacker may record valid communication sent to the TOE and replay all or a portion of the communication to attempt to fool the TOE into performing an unauthorized action or response.	**O.ReplayPrevention** The TOE shall identify and discard any communication that is a replay of previously received communication. **O.Audit** The TOE shall be capable of recording security related events.	O.ReplayPrevention mitigates this threat by identifying and discarding replayed communication. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.

Threat / Policy	Objectives Addressing Threat	Rationale
T.Spoofing An attacker may represent itself as a valid user or device by spoofing the IP address or some other identifying parameter to attempt to compromise the integrity or availability of the TOE or the confidentiality of information in the TOE.	**O.Authentication** The TOE shall be capable of authenticating the identity of a user or device. The TOE shall restrict information access and actions to authenticated users or devices. **O.DataIntegrity** The TOE shall identify if data sent from an authenticated user or device has been modified prior to arriving at the TOE boundary. Modified data shall be rejected. **O.Audit** The TOE shall be capable of recording security related events.	O.Authentication mitigates this threat for new sessions by requiring authentication of the claimed user or device. O.DataIntegrity mitigates this threat for established sessions by requiring verification the communication can from an authenticated source. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.
T.StoredDataAttack An attacker may delete or modify information stored in the TOE to prevent proper operation or to destroy evidence of the TOE.	**O.StoredDataIntegrity** The TOE shall prevent an attacker from modifying or deleting data stored in the TOE. **O.Authentication** The TOE shall be capable of authenticating the identity of a user or device. The TOE shall restrict information access and actions to authenticated users or devices. **O.AccessControl** The TOE shall have an access control capability that restricts information access and operations to authenticated users and devices that are authorized for the requested information access or operation. **O.Audit** The TOE shall be capable of recording security related events.	O.StoredDataIntegrity mitigates this threat by preventing modification or deletion of stored data by an attacker. O.Authentication and O.AccessControl help mitigate this threat by restricted access to authenticated users and devices and providing a means to restrict an authenticated user or device privileges to modify or delete stored data. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.

Threat / Policy	Objectives Addressing Threat	Rationale
T.SystemIntegrity An attacker may attempt to replace or destroy application code,configuration parameters or system data in the TOE to compromise the availability or integrity of the TOE.	**O.ApplicationIntegrity** The TOE shall prevent an unauthorized user or device from modifying or deleting TOE application software. The TOE shall also prevent an unauthorized user or device from modifying the TOE application configuration. **O.SystemIntegrity** The TOE shall prevent unauthorized modification to the operating system software and configuration. **O.SystemDiagnostics** The TOE shall be capable of performing diagnostic tests to verify the integrity of the operating system and application software. **O.SecureStartup** The TOE shall initiate all required security functions prior to accepting requests for information or requests for action. **O.Audit** The TOE shall be capable of recording security related events.	O.ApplicationIntegrity and O.SystemIntegrity mitigate this threat by preventing an attacker from modifying the software or software configuration of the TOE. O.SystemDiagnostics helps mitigate this threat by providing a means to verify system and application integrity. O.SecureStartup helps mitigate this threat by preventing access to the TOE before security functions are up and running. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.

Threat / Policy	Objectives Addressing Threat	Rationale
T.UnauthenticatedAccess An attacker may bypass the authentication mechanism to attempt to compromise the integrity or availability of the TOE or the confidentiality of information in the TOE.	**O.ApplicationIntegrity** The TOE shall prevent an unauthorized user or device from modifying or deleting TOE application software. The TOE shall also prevent an unauthorized user or device from modifying the TOE application configuration. **O.SystemIntegrity** The TOE shall prevent unauthorized modification to the operating system software and configuration. **O.Authentication** The TOE shall be capable of authenticating the identity of a user or device. The TOE shall restrict information access and actions to authenticated users or devices. **O.SecureStartup** The TOE shall initiate all required security functions prior to accepting requests for information or requests for action. **O.Audit** The TOE shall be capable of recording security related events.	O.ApplicationIntegrity and O.SystemIntegrity help mitigate this threat by preventing an attacker from modifying the software or software configuration of the TOE. O.Authentication helps mitigate this threat by limiting access to authenticated users. O.SecureStartup helps mitigate this threat by preventing access to the TOE before security functions are up and running. O.SecureStartup helps mitigate this threat by preventing access to the TOE before security functions are up and running. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.

Threat / Policy	Objectives Addressing Threat	Rationale
T.UnauthorizedAction An attacker that has been authenticated may attempt to perform an unauthorized action by circumventing security in the access control mechanisms.	**O.AccessControl** The TOE shall have an access control capability that restricts information access and operations to authenticated users and devices that are authorized for the requested information access or operation. **O.RoleBasedAccessControl** The TOE shall be capable of placing users and devices into roles and assigning authorization rights to the roles. The TOE shall support at a minimum an Administrator role and an Operator role. **O.ApplicationIntegrity** The TOE shall prevent an unauthorized user or device from modifying or deleting TOE application software. The TOE shall also prevent an unauthorized user or device from modifying the TOE application configuration. **O.SystemIntegrity** The TOE shall prevent unauthorized modification to the operating system software and configuration. **O.SecureStartup** The TOE shall initiate all required security functions prior to accepting requests for information or requests for action. **O.Audit** The TOE shall be capable of recording security related events.	O.AccessControl mitigates this threat by providing controls that define and limit users and devices to authorized actions. O.RoleBasedAccessControl is a specific type of access control that makes it easier to manage user authorizations. O.ApplicationIntegrity and O.SystemIntegrity help mitigate this threat by preventing an attacker from modifying the software or software configuration of the TOE. O.Audit helps mitigate this threat by providing a record of attacks that can be used in incident response.
P.ApprovedCrypto The TOE shall use FIPS-approved security functions and NIST FIPS validated implementations for all cryptographic functions including key management, hashing, encryption, digital signatures, and random number generation.	**OE.StandardCrypto** The TOE shall use cryptologic algorithms and protocols that meet current NIST standards.	OE.StandardCrypto addresses this organizational policy by requiring the TOE use crypto algorithms and protocols that meet current NIST standards.

Threat / Policy	Objectives Addressing Threat	Rationale
P.BackgroundCheck The organization shall insure that users pass a background check prior to having access to the TOE.	**OE.BackgroundCheck** All users shall undergo a background check consistent with the organizations policies and compliant with any applicable laws prior to be given a userID and credentials that provide access to the TOE.	OE.BackgroundCheck addresses this organizational policy by requiring a background check prior to TOE access.
P.Communication The organization shall insure communication to and from the TOE is available.	**OE.ReliableCommunication** Communication between the TOE and authorized subjects shall be reliable.	OE.ReliableCommunication addresses this organization policy by placing a requirement for reliable communications on the operating environment.